

Secure NFC Communication in Mobile Payments: Evaluating Privacy and Authentication in Tap-to-Pay Systems

Nolwazi Ndlovu, Khutso Lebea

Academy of Computer Science and Software Engineering, University of Johannesburg

Johannesburg, South Africa

225051072@student.uj.ac.za, klebea@uj.ac.za

Abstract—This paper examines the security of Near Field Communication (NFC) technology in mobile payment systems, with a focus on tap-to-pay transactions across different device platforms. It describes how NFC operates within mobile payments and identifies key vulnerabilities that can arise during real-world use, such as relay attacks, token theft, backend compromise, and biometric spoofing. The work also reviews and compares existing authentication mechanisms and security frameworks, assessing their effectiveness in mitigating these risks. Through the lens of a practical case study, the analysis connects technical concepts to realistic threat scenarios, highlighting recurring security challenges, platform-specific differences, and areas where improvements are still needed. The purpose is to provide a clear, evidence-based understanding of how NFC security measures function in practice and how they address or fail to address the most pressing privacy and authentication concerns in current mobile payment deployments.

Keywords—Near Field Communication, Mobile Payments, Authentication, Privacy, Security Frameworks

I. INTRODUCTION

Near Field Communication (NFC) has emerged as a cornerstone of modern mobile payment ecosystems, enabling short-range, contactless transactions that combine speed, convenience, and integration across devices and platforms. Tap-to-pay functionality, now widely adopted across Android, iOS, and legacy mobile devices, has transformed consumer payment behaviour by reducing transaction times and eliminating the need for physical card handling [1, 2]. However, the same characteristics that make NFC payments attractive, short interaction times, wireless communication, and integration with multiple backend systems also expose them to a range of privacy and authentication vulnerabilities [3, 4].

There are two reasons why this topic was chosen. First, the attack surface for adversaries has been greatly increased by the adoption of mobile payment apps like Apple Pay, Google Wallet, and Samsung Pay [2, 5]. Second, the scholarly literature shows that traditional authentication methods like static passwords and PINs are continuously evolving in favour of new NFC security frameworks that integrate formal verification, advanced cryptography, dynamic authentication, and privacy-preserving design principles [6, 4, 7]. This change represents a move away from single-layer, reactive defences and towards layered, proactive structures.

Studies identifies several broad themes:

- **Recurring Attack Vectors:** Relay attacks, token theft/reuse, backend compromise, session key weaknesses, and biometric spoofing appear across all platform types and architectures [8, 1].
- **Architectural Trade-offs:** Hardware-secured models, such as Secure Element (SE) in iOS, offer strong local protection but cannot fully prevent backend or cloud-based threats. In contrast, software-based Host Card Emulation (HCE) improves flexibility and compatibility but exposes critical credentials to the operating system environment [2, 9].
- **Innovation Trends:** Emerging frameworks increasingly integrate elliptic curve cryptography (ECC), AES-GCM encryption, offline session key generation with MAC and hash functions, gesture-based biometric authentication, and behavioural analytics to resist a broader range of threats [6, 4, 7, 10].
- **Verification and Efficiency:** Formal verification (e.g., ProVerif, BAN logic) and lightweight cryptography are widely adopted to maintain resource efficiency while ensuring provable security guarantees [11, 12].

Despite this progress, several gaps remain. Many studies rely on simulation or controlled laboratory environments without field deployment data [6, 4], limiting external validity. There is also a lack of standardised, cross-platform benchmarks for measuring privacy preservation and authentication robustness, particularly in mixed environments where hardware-secured and software-secured devices coexist. Furthermore, the integration of privacy-preserving features with usability remains challenging; multi-layered security can introduce authentication delays or user friction that impede adoption [7, 10].

Problem Statement: While traditional authentication mechanisms provide a baseline for NFC payment security, they fail to adequately address evolving data breach risks posed by sophisticated attack vectors. Emerging NFC security frameworks claim to offer higher levels of protection through advanced cryptography, formal verification, and multi-factor

authentication, yet their comparative effectiveness across different platforms and against diverse threat models has not been comprehensively quantified. This creates uncertainty for payment providers, regulators, and consumers when selecting or endorsing specific architectures.

To address this problem, this paper investigates the extent to which emerging NFC security frameworks mitigate potential data breach risks compared to existing authentication mechanisms in mobile payment systems. The analysis draws from relevant screened studies, focusing on tap-to-pay scenarios across Android, iOS, and legacy platforms.

Paper Structure: Section 2 presents a detailed case study of a supermarket tap-to-pay transaction, identifying threats and platform-specific risks. Section 3 outlines the technical background, including NFC architectures, privacy vulnerabilities, and authentication weaknesses. Section 4 expands on the threat landscape, categorising attacks by mechanism and impact. We survey prominent NFC security frameworks, including NSPMT, privacy-preserving protocols, gesture-based biometrics, TSM-centric models, POSAUTH, and the Trusted Tapping Protocol. We will also provide a comparative evaluation of these frameworks, leading to the proposal of a hybrid model that integrates their respective strengths. while Section 5 concludes with key findings and recommendations.

II. CASE STUDY: TAP-TO-PAY AT RETAIL CHECKOUT

A. Scenario Overview

This case study examines a common use of Near Field Communication (NFC) in mobile payments: a tap-to-pay transaction at a supermarket point-of-sale (POS) terminal. The customer initiates the payment by bringing their smartphone within approximately 4 cm of the terminal, establishing a wireless link compliant with ISO/IEC 14443 standards. Depending on the platform and configuration, the interaction may rely on:

- **Host Card Emulation (HCE):** A software-based emulation of a payment card, with credentials stored in the mobile operating system environment [1].
- **Secure Element (SE):** A tamper-resistant hardware module embedded in the device (e.g., Apple's Secure Enclave) or on a Universal Integrated Circuit Card (UICC) [2].
- **Hybrid Architectures:** Combining HCE flexibility with SE-protected storage for certain credentials [4].

While the transaction lasts only a few seconds, several complex processes occur: device and terminal negotiate capabilities, exchange authentication data, and trigger backend payment authorisation. These operations involve local NFC radio communication, cryptographic exchanges, token generation, and potentially cloud synchronisation of credentials.

B. Threat Landscape in the Scenario

Insights from the studies show multiple vulnerabilities that can arise during this process:

- **Relay Attacks:** Also known as “Mafia fraud,” this involves two colluding devices, one near the victim, one

near the legitimate terminal to extend the communication range and impersonate the victim without physical theft of their device [8, 2]. Studies confirm successful proof-of-concept demonstrations on Android HCE and theoretical feasibility on SE-based systems.

- **Token Misuse and Lifting:** Poorly implemented tokenisation can result in static or long-lived tokens that attackers can extract from device memory or intercept during transmission, then reuse to authorise fraudulent transactions [5, 1].
- **Backend Exploits:** Even when NFC channel security is intact, cloud synchronisation, API endpoints, and Trusted Service Manager (TSM) provisioning may be susceptible to phishing, SIM-swapping, or man-in-the-middle attacks on backend links [4, 13].
- **Biometric Spoofing:** Where biometric verification (e.g., fingerprint or face ID) is employed, spoofing attacks or replayed biometric data may be used to bypass user authentication [7].

C. Platform-Specific Risks

Evidence across platforms indicates differing exposure:

- **Android:** HCE-based implementations expose credentials to the OS and application layer, making them vulnerable to malware or malicious apps exploiting NFC APIs without privileged access [1].
- **iOS:** SE-based architecture provides stronger local protection, but Alamleh et al. [2] report backend/cloud vulnerabilities including token retrieval and phishing-based credential compromise.
- **Legacy Devices:** Older platforms (e.g., BlackBerry, Nokia) show SE access control flaws and susceptibility to denial-of-service (DoS) during NFC initialisation [9].

D. Issues Highlighted for the Paper

This case study crystallises the key issues that the rest of this paper addresses:

- 1) How emerging NFC frameworks such as NSPMT [6], privacy preserving protocols [4], gesture-based biometrics [7], and Trusted Tapping Protocol [2] defend against relay, token theft, and backend exploitation.
- 2) The trade-offs between hardware-secured (SE) and software-based (HCE) designs in mitigating identified risks.
- 3) Quantifying the improvement in authentication robustness and privacy protection when moving from legacy or traditional mechanisms to modern, multi-layered frameworks.

III. BACKGROUND

A. NFC Architecture in Mobile Payments

Near Field Communication (NFC) operates on ISO/IEC 14443 and ISO/IEC 18092 standards, enabling secure data exchange over distances typically less than 4 cm. In retail tap-to-pay scenarios, such as the supermarket checkout example, three primary architectural models are used:

- **Host Card Emulation (HCE):** Implements payment card emulation entirely in software, relying on the device's OS to store and process credentials [1]. This model offers flexibility and low hardware requirements but exposes sensitive data to the host environment.
- **Secure Element (SE):** A tamper-resistant hardware component (embedded, SIM-based, or microSD) that stores cryptographic keys and executes sensitive operations in isolation [2]. Used by Apple Pay, it limits OS-level exposure but still depends on backend security.
- **Trusted Service Manager (TSM):** A backend service provisioning and managing credentials in SEs across devices and platforms [13]. In the supermarket example, TSM handles token distribution when a user first sets up their payment method.

These architectures may be deployed individually or in hybrid configurations. In the case study, a customer using Google Wallet on Android would employ HCE, while an iPhone customer would use an SE-based flow.

B. Privacy Vulnerabilities in NFC Payments

The studies identifies privacy risks arising both locally (device-POS communication) and remotely (backend systems):

- **Data Leakage:** If NFC payloads or metadata are insufficiently encrypted, adversaries can intercept transaction data using specialised equipment within range of the POS [1].
- **Tracking via Identifiers:** Persistent IDs or static tokens allow merchants or malicious third parties to correlate transactions over time [4].
- **Backend Data Exposure:** Cloud token synchronisation, TSM compromise, or misconfigured APIs can leak user account details even when the NFC channel is secure [13].

In the supermarket case study, an attacker positioned near the POS could capture unencrypted identifiers during the handshake, enabling profiling of a customer's shopping habits.

C. Authentication Weaknesses

Authentication ensures the payer is authorised to initiate the NFC transaction. Weaknesses documented across the studies include:

- **Relay Attacks:** Adversaries use two devices to extend NFC range, effectively bypassing proximity-based trust [8, 2].
- **Token Reuse or Lifting:** Stolen or intercepted tokens—particularly static ones—can be replayed for fraudulent purchases [5].
- **Session Key Flaws:** Weak generation or absence of key rotation enables replay or impersonation attacks in successive transactions [4].
- **Biometric Spoofing:** Gesture or facial recognition mechanisms without sufficient liveness detection can be circumvented [7].

In the checkout scenario, a relay attack could involve a proxy phone near the victim's bag transmitting signals to an accomplice's phone at a rogue POS.

D. Platform-Specific Risk Analysis

The severity and type of vulnerabilities vary by platform:

- **Android (HCE):** Open NFC stack and software token storage increase exposure to malware, relay attacks, and token lifting [1].
- **iOS (SE):** Hardware isolation prevents OS-level theft, but backend and cloud-based vulnerabilities persist [2].
- **Legacy Devices:** Older Nokia, BlackBerry, and Samsung models with embedded SEs show flawed access controls and are prone to Denial-of-Service attacks during NFC initialization [9].

These differences influence the choice and effectiveness of security frameworks examined later in this paper.

In the supermarket tap-to-pay example, the background concepts manifest as follows:

- The NFC architecture determines whether sensitive keys are exposed to the OS or isolated in hardware.
- Privacy vulnerabilities could arise from transaction metadata captured by malicious nearby devices.
- Authentication weaknesses such as relay attacks threaten both HCE and SE flows.
- Platform-specific differences explain why the same attack vector may succeed on one device class but fail on another.

IV. DISCUSSION, COMPARATIVE EVALUATION, AND FRAMEWORK PROPOSAL

The analysis of NFC tap-to-pay technologies reveals a consistent set of vulnerabilities across Android, iOS, and legacy platforms. Relay attacks, token lifting, backend compromise, and biometric spoofing represent the most persistent threats, with varying severity depending on architectural design. In the supermarket checkout scenario, these vulnerabilities manifest in ways that demonstrate both the sophistication of current attack vectors and the limitations of existing countermeasures.

A. Framework Performance and Trade-offs

Six prominent frameworks from the literature were assessed for their capacity to mitigate the identified threats:

- **NSPMT** [6] applies a defense-in-depth strategy with elliptic curve cryptography (ECC), AES-GCM encryption, and formal verification. It scores highly on cryptographic strength and verified protocol soundness, with demonstrated resistance to relay and token-reuse attacks.
- **Privacy-Preserving Protocols** [4] emphasise offline session key generation, MAC-based authentication, and hash chaining. They offer strong privacy guarantees and resilience to tracking and replay, though deployment complexity and user transparency remain considerations.

- **Gesture-Based Biometrics** [7] authenticate transactions using device motion sensors and machine learning classifiers. While highly usable and resistant to certain spoofing attacks, their cryptographic coverage is limited, and performance may degrade with sensor inconsistencies.
- **TSM-Centric Privacy Models** [13] remove sensitive data from merchant systems and rely on secure backend provisioning. They address backend compromise risks effectively but depend on robust TSM infrastructure and governance.
- **POSAUTH Protocol** [5] uses ephemeral keys and mutual authentication to protect against relay and replay attacks. Its theoretical strength is high, though real-world deployment evidence is limited.
- **Trusted Tapping Protocol (TTP)** [2] uses tap patterns, proximity cues, and environmental sensing to verify intent, showing strong empirical resistance to relay attacks without imposing significant transaction delays.

B. Comparative Evaluation

Table I consolidates the cross-framework comparison against four key dimensions drawn from the studies: cryptographic strength, privacy protection, usability, and formal verification.

TABLE I
COMPARATIVE EVALUATION OF NFC SECURITY FRAMEWORKS

Framework	Crypto Strength	Privacy	Usability	Verification
NSPMT [6]	High	Moderate	High	Formal
Privacy-Preserving [4]	Moderate	High	Moderate	Formal
Gesture Biometrics [7]	Low	Moderate	High	Empirical
TSM-Centric [13]	High	High	Moderate	Formal
POSAUTH [5]	High	Moderate	Moderate	Theoretical
TTP [2]	Moderate	High	High	Empirical

The comparative results indicate that no single framework dominates all categories. Hardware-reliant models such as NSPMT and TSM-Centric protocols excel in cryptographic assurance, whereas Privacy-Preserving and TTP approaches provide superior privacy safeguards. Gesture biometrics lead in usability but lack formal cryptographic rigor.

C. Hybrid Model Proposal

Given the complementary strengths identified, a hybrid framework is proposed that integrates:

- 1) **Cryptographic Core:** ECC for key exchange and AES-GCM for payload encryption, ensuring strong confidentiality and integrity.
- 2) **Privacy Layer:** MAC anonymisation and hash chaining to decouple user identity from transaction metadata and prevent tracking.
- 3) **User Authentication:** Gesture-based biometric verification using accelerometer and gyroscope data to confirm physical presence and resist relay exploitation.
- 4) **Backend Assurance:** TSM-managed provisioning with formal verification (ProVerif) to secure credential life-cycle and prevent backend compromise.

D. Implementation Considerations

The hybrid model's modular architecture supports deployment across diverse hardware environments, from SE-equipped iOS devices to HCE-dependent Android systems. Its layered design reduces single points of failure: even if biometric verification is bypassed, cryptographic and backend safeguards remain in place. Lightweight cryptographic primitives and transparent biometrics address latency and usability concerns, while formal verification provides confidence in security claims.

E. Anticipated Impact

By combining high-assurance cryptography, privacy-preserving protocols, behavioural authentication, and verified backend processes, the hybrid model aims to reduce the likelihood of successful relay, token misuse, and backend attacks by a significant margin compared to legacy mechanisms. While empirical field validation remains a gap across much of the literature, simulation and controlled trials of similar component frameworks report high detection accuracy and low resource overheads.

This integrated approach directly responds to the threats identified in the case study and addresses the architectural trade-offs observed across current NFC mobile payment systems, positioning it as a viable candidate for standardisation and cross-platform adoption.

V. CONCLUSION AND FUTURE WORK

This study set out to answer the research question: *To what extent do emerging NFC security frameworks mitigate potential data breach risks compared to existing authentication mechanisms in mobile payment systems?* The findings demonstrate that emerging frameworks consistently outperform traditional single-factor or static credential systems on multiple fronts.

In the supermarket tap-to-pay case study, threats such as relay attacks, token lifting, backend compromise, and biometric spoofing were shown to affect all platform types, albeit in different ways. Comparative analysis of six representative frameworks: NSPMT [6], Privacy-Preserving Protocols [4], Gesture-Based Biometrics [7], TSM-Centric Privacy Models [13], POSAUTH [5], and the Trusted Tapping Protocol [2] revealed that no single design dominates across all criteria. Instead, distinct strengths emerge: high cryptographic assurance from ECC/AES-GCM-based models, strong privacy from MAC and hash-chained protocols, high usability from sensor-driven biometrics, and proven backend isolation from TSM-centric approaches.

The proposed hybrid model integrates these complementary features into a layered, modular architecture, offering:

- End-to-end cryptographic protection with ECC key exchange and AES-GCM encryption.
- Privacy-preserving transaction metadata handling via MAC anonymisation and hash chaining.
- Behavioural authentication through gesture biometrics to verify transaction intent.

- Backend assurance through formally verified provisioning and credential lifecycle management.

Such integration directly addresses the vulnerabilities observed in current deployments and balances security, privacy, and usability without introducing prohibitive computational overhead.

However, several gaps remain. Most included studies validated their protocols in simulation or controlled environments; real-world deployment data is scarce. Interoperability challenges persist in mixed HCE/SE/TSM environments, and multi-layer security can introduce latency or usability trade-offs that may hinder adoption if not carefully optimised.

Future Work should focus on:

- 1) Field trials of integrated frameworks in live merchant environments to obtain empirical performance and adoption data.
- 2) Adaptive, context-aware authentication that adjusts security levels based on transaction value, geolocation, or detected anomalies.
- 3) Exploration of federated learning to personalise gesture or behavioural models while preserving user privacy.
- 4) Formal verification of hybrid and adaptive protocols to prove robustness against evolving threats, including those posed by post-quantum adversaries.

By combining rigorous cryptography, privacy-by-design, and context-aware authentication, emerging NFC security frameworks show clear potential to significantly reduce data breach risks compared to legacy authentication methods. The trajectory of research suggests that the next generation of NFC payment security will depend on modular, adaptable designs that can evolve alongside both technology and threat landscapes.

REFERENCES

- [1] Maurizio Cavallari, L. Adami, and Francesco Torniery. Organisational aspects and anatomy of an attack on nfc/hce mobile payment systems. In *International Conference on Enterprise Information Systems*, pages 421–430, 2015.
- [2] H. Alamleh, S. Jafarikhah, and B. Al Smadi. Trusted tapping protocol for nfc authentication. In *International Conference Radioelektronika*, pages 12–26, 2025.
- [3] Nicholas Akinyokun and Vanessa Teague. Security and privacy implications of nfc-enabled contactless payment systems. In *International Conference on Availability, Reliability and Security (ARES)*, 2017.
- [4] Ali M. Allam. Privacy-preserving nfc-based authentication protocol for mobile payment system. *KSII Transactions on Internet and Information Systems*, 9(2):87–102, 2023.
- [5] Xiaolong Bai, Zhe Zhou, Xiaofeng Wang, Zhou Li, Xianghang Mi, N. Zhang, Tongxin Li, Shimin Hu, and Kehuan Zhang. Picking up my tab: Understanding and mitigating synchronized token lifting and spending in mobile payment. In *USENIX Security Symposium*, pages 1–16, 2017.
- [6] S. Ahamad et al. Nspmt: A secure nfc mobile transaction framework. *Journal of Mobile Security*, 14(3):145–158, 2022.
- [7] B. Shrestha, M. Mohamed, S. Tamrakar, and N. Saxena. Theft-resilient mobile wallets: Transparently authenticating nfc users with tapping gesture biometrics. In *Asia-Pacific Computer Systems Architecture Conference*, pages 33–42, 2016.
- [8] Maryam Mehrnezhad, Feng Hao, and Siamak F. Shahandashti. Tap-tap and pay (ttp): Preventing the mafia attack in nfc payment. In *ACM SIGSOFT Symposium on Software Reusability*, pages 33–42, 2015.
- [9] Michael Roland, Josef Langer, and Josef Scharinger. Practical attack scenarios on secure element-enabled mobile devices. In *4th International Workshop on Near Field Communication*, pages 19–24, 2012.
- [10] Dirar Abu-Saymeh, D. E. D. I. Abou-Tair, and Ahmad Zmily. An application security framework for near field communication. In *12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, pages 1–8, 2013.
- [11] Chalee Thammarat. Efficient and secure nfc authentication for mobile payment ensuring fair exchange protocol. *Symmetry*, 12(4):1–15, 2020.
- [12] Munefah Alshammari and S. Nashwan. Fully authentication services scheme for nfc mobile payment systems. *Intelligent Automation and Soft Computing*, 32(1):145–160, 2022.
- [13] K. Ammayappan. Tsm centric privacy preserving nfc mobile payment framework with formal verification. In *International Conference on Electronics, Circuits, and Systems*, 2015.